REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application. Claims 1-21 are pending in this application.

35 U.S.C. § 103

Claims 1-5, 7, 9-13, 15, and 17-18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,944,821 to Angelo (hereinafter "Angelo") in view of Arbaugh and further in view of U.S. Patent No. 5,974,546 to Anderson (hereinafter "Anderson"). Applicant respectfully submits that claims 1-5, 7, 9-13, 15, and 17-18 are not obvious over Angelo in view of Arbaugh and further in view of Anderson.

As discussed in the Abstract of Angelo, Angelo is directed to a method for providing secure registration and integrity assessment of software in a computer system. A secure hash table is created containing a list of secure programs that the user wants to validate prior to execution. The table contains a secure hash value (i.e., a value generated by modification detection code) for each of these programs as originally installed on the computer system. This hash table is stored in protected memory that can only be accessed when the computer system is in system management mode. Following an attempt to execute a secured program, a system management interrupt is generated. An SMI handler then generates a current hash value for the program to be executed. In the event that the current hash value matches the stored hash value, the integrity of the program is guaranteed and it is loaded into memory and executed. If the two values do not

match, the user is alerted to the discrepancy and may be given the option to update or override the stored hash value by entering an administrative password.

Arbaugh, as discussed in section 1.1, 1st paragraph, is directed to a system referred to as AEGIS. AEGIS ensures the integrity of the bootstrap code by constructing a chain of integrity checks, beginning at power-on and continuing until the final transfer of control from the bootstrap components to the operating system itself. The integrity checks compare a computed cryptographic hash value with a stored digital signature associated with each component.

Anderson is directed to a method for determining the cause of an unsuccessful boot attempt to improve the probability of a successful subsequent boot attempt (see, col. 1, lines 9-12). Anderson discusses a status flag called INPOST that indicates whether the previous attempt to boot the system failed (see, col. 5, lines 17-19). If the INPOST flag is set, then the previous attempt to boot the system failed (see, col. 5, lines 19-21). If the INPOST flag is not set, then the previous attempt to boot succeeded (see, col. 5, lines 21-22).

With respect to claim 1, claim 1 recites:

> In a computer system having a central processing unit (CPU) and an operating system (OS), the CPU having a software identity register, a method for booting the operating system comprising:
>
> computing a cryptographic function of at least a portion of the operating system; and
>
> setting the software identity register to a result of the computed cryptographic function if atomic execution of a boot block of the operating system does not fail, and otherwise setting the software identity register to a value indicating that the atomic execution of the boot block failed.

Applicant respectfully submits that Angelo in view of Arbaugh and further in view of Anderson does not disclose or suggest such setting as recited in claim 1.

As seen in claim 1, the same software identity register is set to one of two different values: the result of the computed cryptographic function if atomic execution of the boot block of the operating system does not fail, and a value indicating that the atomic execution of the boot block failed if atomic execution of the boot block of the operating system does fail. Applicant respectfully submits that no such setting is disclosed or suggested by Angelo in view of Arbaugh and further in view of Anderson.

In the November 1, 2005 Office Action at p. 3, it was asserted that:

> Arbaugh discloses a system that verifies the kernel (operating system) by calculating the cryptographic and storing the hash of the operating system level (page 4 section 3.2.1 paragraph 2 in combination with section 3.2.2 paragraph 4). The cryptographic hash is the identity of the operating system since it is used to verify the integrity of the system.

Arbaugh at section 3.2.1 paragraph 2 recites:

> The transition between levels in a traditional boot process is accomplished with a jump or a call instruction without any attempt at verifying the integrity of the next level. AEGIS, on the other hand, uses public key cryptography and cryptographic hashes to protect the transition from each lower level to the next higher one, and its recovery process ensures the integrity of the next level in the event of failures.

Arbaugh at section 3.2.2 paragraph 4 recites:

> Assuming that the boot block is verified successfully, control is passed to it (Level 3). If a secondary boot block is required, then it is verified by the primary block before passing control to it. Finally, the kernel is verified by the last boot block in the chain before passing control to it (Level 4).

However, nowhere does Arbaugh discuss setting a particular register (the software identity register) to a result of a computed cryptographic function if atomic

execution of a boot block of the operating system does not fail. Arbaugh discusses passing control to a next level if the boot block is verified, but not setting a particular register to a result of a computed cryptographic function if atomic execution of a boot block of the operating system does not fail.

In the November 1, 2005 Office Action at p. 4, it was further asserted that:

> Anderson discloses a system wherein if the atomic execution of the boot block does not fail, and otherwise setting the software identity register to a value indicating that the atomic execution of the boot block failed (column 5 lines 34-41).

Anderson at column 5, lines 34-41 recites:

> At block 110, the INPOST flag is set as a determiner, in case the present system boot sequence fails. If the present attempt to boot the system ultimately fails, then the INPOST flag will indicate that on the subsequent boot. However, as will be described later, if this present attempt to boot progresses to the end and succeeds, then the INPOST flag will be reset. Thereby, during a subsequent boot attempt, the INPOST flag will indicate that this boot attempt succeeded.

However, nowhere in Angelo, Arbaugh, or Anderson is there any discussion or mention of having a single software identity register that is set to a cryptographic hash of Arbaugh under certain circumstances and is set as a determiner of Anderson under other circumstances. Without any such discussion or mention, Applicant respectfully submits that Angelo in view of Arbaugh and further in view of Anderson cannot disclose or suggest the setting of a single software identity register to different values under different conditions as recited in claim 1.

For at least these reasons, Applicant respectfully submits that claim 1 is allowable over Angelo in view of Arbaugh and further in view of Anderson.

With respect to claim 2, given that claim 2 depends from claim 1, Applicant respectfully submits that claim 2 is likewise allowable over Angelo in view of Arbaugh for at least the reasons discussed above with respect to claim 1.

With respect to claim 3, Applicant respectfully submits that, similar to the discussion above regarding claim 1, Angelo in view of Arbaugh and further in view of Anderson does not disclose or suggest executing an atomic operation to set an identity of the operating system into the software identity register of the CPU, wherein in an event that the atomic operation completes correctly, the software identity register contains the identity of the operating system and in an event that the atomic operation fails to complete correctly, the software identity register contains a value indicating that the atomic operation failed as recited in claim 3. For at least these reasons, Applicant respectfully submits that claim 3 is allowable over Angelo in view of Arbaugh and further in view of Anderson.

With respect to claim 4, claim 4 depends from claim 3 and Applicant respectfully submits that claim 4 is allowable over Angelo in view of Arbaugh and further in view of Anderson for at least the reasons discussed above with respect to claim 3. Furthermore, claim 4 recites:

> The method as recited in claim 3, wherein the identity comprises a public key of a correctly signed block of code from the operating system, and examining a content of the software identity register comprises verifying a signature of the signed block of code against the public key.

Applicant respectfully submits that Angelo in view of Arbaugh and further in view of Anderson does not disclose or suggest wherein the identity comprises a public key of a correctly signed block of code from the operating system as recited in claim 4.

In the November 1, 2005 Office Action at p. 6, Arbaugh at section 3.2.2 paragraph 2 is cited as disclosing the identity comprises a public key of a correctly signed block of code from the operating system of claim 4. Applicant respectfully disagrees. Arbaugh at section 3.2.2 paragraph 2 recites:

> The first section executes and performs the standard checksum calculation over its address space to protect against ROM failures. Following successful completion of the checksum, the cryptographic hash of the second section is computed and verified against a stored signature. If the signature is valid, control is passed to the second section *i.e.*, Level 1.

Thus, this cited portion of Arbaugh discusses computing a cryptographic hash of a section and verifying it against a stored signature. However, nowhere is there any discussion or mention of the identity of the operating system being a public key, and the software identity register being set to that public key. Simply computing a cryptographic hash of a section does not disclose or suggest setting a software identity register to a public key as recited in claim 4. As such, Applicant respectfully submits that Arbaugh does not disclose or suggest wherein the identity comprises a public key of a correctly signed block of code from the operating system as recited in claim 4.

With respect to Angelo and Anderson, Angelo and Anderson are not cited as curing, and do not cure, these deficiencies of Arbaugh. For at least these reasons, Applicant respectfully submits that claim 4 is allowable over Angelo in view of Arbaugh and further in view of Anderson.

Given that claims 5 and 7 depend from claim 3, Applicant respectfully submits that claims 5 and 7 are likewise allowable over Angelo in view of Arbaugh for at least the reasons discussed above with respect to claim 3.

With respect to claim 9, claim 9 depends from claim 3 and Applicant respectfully submits that claim 9 is allowable over Angelo in view of Arbaugh for at least the reasons discussed above with respect to claim 3. Furthermore, claim 9 recites:

> The method as recited in claim 3, further comprising generating a storage key for encrypting data to be stored on the computer system from a seed based in part on the identity of the operating system.

Applicant respectfully submits that Angelo in view of Arbaugh does not disclose or suggest generating a storage key as recited in claim 9.

In the November 1, 2005 Office Action at p. 6, it was asserted that:

> *In reference to claims 4, 9, 10, 12, 17, and 18,* the identity comprises a public key of a correctly signed block of code from the operating system, and examining a content of the software identity register comprises verifying a signature of the signed block of code against the public key (Section 3.2.2 paragraph 2 Arbaugh).

This rejection of claim 9 does not make any reference to generating a storage key for encrypting data to be stored on the computer system from a seed based in part on the identity of the operating system or where such generating is asserted as being disclosed in Arbaugh, Angelo, or Anderson. Arbaugh at section 3.2.2 paragraph 2 recites:

> The first section executes and performs the standard checksum calculation over its address space to protect against ROM failures. Following successful completion of the checksum, the cryptographic hash of the second section is computed and verified against a stored signature. If the signature is valid, control is passed to the second section *i.e.*, Level 1.

Thus, it can be seen that Section 3.2.2 paragraph 2 of Arbaugh does not include any discussion or mention of generating storage keys, much less of generating a storage key for encrypting data to be stored on the computer system from a seed

based in part on the identity of the operating system as recited in claim 9. Without any such discussion or mention, Applicant respectfully submits that Arbaugh cannot disclose or suggest generating a key as recited in claim 9.

With respect to Angelo and Anderson, Angelo and Anderson are not cited as curing, and do not cure, these deficiencies of Arbaugh. For at least these reasons, Applicant respectfully submits that claim 9 is allowable over Angelo in view of Arbaugh and further in view of Anderson.

Given that claim 10 depends from claim 9, Applicant respectfully submits that claim 10 is likewise allowable over Angelo in view of Arbaugh for at least the reasons discussed above with respect to claim 9.

With respect to claim 11, Applicant respectfully submits that, similar to the discussion above regarding claim 1, Angelo in view of Arbaugh does not disclose or suggest executing an atomic operation to set the identity of the operating system into the software identity register of the CPU, wherein in an event that the atomic operation completes correctly, the software identity register is set to contain the identity of the operating system, and in an event that the atomic operation does not complete correctly, the software identity register is set to contain a false value to indicate failure of the atomic operation as recited in claim 11. For at least these reasons, Applicant respectfully submits that claim 11 is allowable over Angelo in view of Arbaugh and further in view of Anderson.

With respect to claim 12, claim 12 depends from claim 11 and Applicant respectfully submits that claim 12 is allowable over Angelo in view of Arbaugh and further in view of Anderson for at least the reasons discussed above with respect to claim 11. Furthermore, Applicant respectfully submits that, similar to

the discussion above regarding claim 4, Angelo in view of Arbaugh and further in view of Anderson does not disclose or suggest the signature and a corresponding public key from the key pair forming the OS identity as recited in claim 12. For at least these reasons, Applicant respectfully submits that claim 12 is allowable over Angelo in view of Arbaugh and further in view of Anderson.

Given that claims 13 and 15 depend from claim 11, Applicant respectfully submits that claims 13 and 15 are likewise allowable over Angelo in view of Arbaugh and further in view of Anderson for at least the reasons discussed above with respect to claim 11.

With respect to claim 17, claim 17 depends from claim 11 and Applicant respectfully submits that claim 17 is allowable over Angelo in view of Arbaugh and further in view of Anderson for at least the reasons discussed above with respect to claim 11. Furthermore, Applicant respectfully submits that, similar to the discussion above regarding claim 9, Angelo in view of Arbaugh and further in view of Anderson does not disclose or suggest generating a storage key for encrypting data to be stored on the computer system from a seed based in part on the identity of the OS as recited in claim 17. For at least these reasons, Applicant respectfully submits that claim 17 is allowable over Angelo in view of Arbaugh and further in view of Anderson.

Given that claim 18 depends from claim 17, Applicant respectfully submits that claim 18 is likewise allowable over Angelo in view of Arbaugh and further in view of Anderson for at least the reasons discussed above with respect to claim 17.

Claims 6, 8, 14, 16, and 21 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Angelo, Arbaugh, and Anderson, and further in view of U.S.

Patent No. 6,230,286 to Sadowsky et al. (hereinafter "Sadowsky") in view of Arbaugh. Applicant respectfully submits that claims 6, 8, 14, 16, and 21 are not obvious over Angelo in view of Arbaugh and Anderson and further in view of Sadowsky.

As discussed in the Abstract of Sadowsky, Sadowsky is directed to a boot failure recovery system that operates to diagnose a failed system boot in a computer operating system which boots by bootstrapping from a boot sector of a storage medium using configuration information. The boot failure recovery system includes an agent which monitors operating system files used during system boot and which stores information regarding changes to the system files to a change file. A repair module analyzes the change file to determine the cause of the failed system boot. A boot check module responds to initiation of a system boot by determining if a prior system boot was successful. The boot check module causes execution of a first boot sector code module upon occurrence of a successful prior system boot and causes execution of the repair module upon occurrence of a failed prior system boot.

With respect to claims 6 and 8, claims 6 and 8 depend from claim 3 and Applicant respectfully submits that claims 6 and 8 are allowable over Angelo in view of Arbaugh and Anderson for at least the reasons discussed above with respect to claim 3. Sadowsky is not cited as curing, and does not cure, the deficiencies of Angelo in view of Arbaugh and Anderson discussed above with respect to claim 3. Accordingly, for at least these reasons, Applicant respectfully submits that claims 6 and 8 are allowable over Angelo in view of Arbaugh and Anderson and further in view of Sadowsky.

With respect to claims 14 and 16, claims 14 and 16 depend from claim 11 and Applicant respectfully submits that claims 14 and 16 are allowable over Angelo in view of Arbaugh and Anderson for at least the reasons discussed above with respect to claim 11. Sadowsky is not cited as curing, and does not cure, the deficiencies of Angelo in view of Arbaugh and Anderson discussed above with respect to claim 11. Accordingly, for at least these reasons, Applicant respectfully submits that claims 14 and 16 are allowable over Angelo in view of Arbaugh and Anderson and further in view of Sadowsky.

With respect to claim 21, claim 21 depends from claim 19. In the November 1, 2005 Office Action at p. 10, it was acknowledged that Arbaugh does not disclose a verification system that uses certificates. Angelo, Anderson, and Sadowsky are not cited as curing, and do not cure, this deficiency of Arbaugh. Accordingly, for at least these reasons, Applicant respectfully submits that claim 21 is allowable over Angelo in view of Arbaugh and Anderson and further in view of Sadowsky.

Claim 19 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Angelo in view of Arbaugh and further in view of "Cryptography and Network Security" to Stallings (hereinafter "Stallings"). Applicant respectfully submits that claim 19 is not obvious over Angelo in view of Arbaugh and further in view of Stallings.

With respect to claim 19, claim 19 recites:

> In a computer system having a central processing unit (CPU) and an operating system (OS), the CPU having a pair of private and public keys and a software identity register that holds an identity of the operating system, a method comprising:

creating an OS certificate including the identity from the software identity register, information describing the operating system, and the CPU public key; and

signing the OS certificate using the CPU private key.

Applicant respectfully submits that Angelo in view of Arbaugh and further in view of Stallings does not disclose such creating and signing.

In the November 1, 2005 Office Action at p. 10, it was asserted that:

> At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize digital certificates for the verification process of Stalling instead of the system disclosed by Arbaugh. One of ordinary skill in the art would have been motivated to do this because any participant can verify that the certificate originated from the certificate authority and is not counterfeit.

However, Applicant respectfully submits that, even if Arbaugh and Stalling were combined, the combination still does not disclose or suggest the creating and signing of claim 19. Claim 19 recites **creating an OS certificate including the identity from the software identity register**. Arbaugh discusses that the cryptographic hash of the second section is computed and verified against a stored signature (see, section 3.2.2 paragraph 2). But nowhere does Arbaugh disclose or suggest creating anything that includes the identity from a software identity register. Thus, even if combined with Stalling, there still would be no disclosure or suggestion of creating an OS certificate including the identity from the software identity register as recited in claim 19.

Furthermore, claim 19 recites creating an OS certificate including the identity from the software identity register, **information describing the operating system**, and the CPU public key. Thus, the OS certificate created in claim 19 includes, in addition to the identity from the software identity register, information describing the operating system. Nowhere in Arbaugh, Angelo, or Stalling is there

any discussion or mention of including such information describing the operating system in an OS certificate as recited in claim 19. As such, Applicant respectfully submits that Angelo in view of Arbaugh and further in view of Stallings does not disclose or suggest the creating and signing of claim 19.

For at least these reasons Applicant respectfully submits that claim 19 is allowable over Angelo in view of Arbaugh and further in view of Stallings.

Claim 20 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Angelo in view of Arbaugh and Stallings and further in view of U.S. Patent No. 6,026,166 to LeBourgeois et al. (hereinafter "LeBourgeois"). Applicant respectfully submits that claim 20 is not obvious over Angelo in view of Arbaugh and Stallings and further in view of LeBourgeois.

As discussed in the Abstract of LeBourgeois, LeBourgeois is directed to a digital certification method in which a first digital signature dependent upon a first user identity and a first user system in combination, is stored accessibly to a certification server. The first user identity can be distinguished by, for example, a PIN provided by the user. Subsequently, the user system generates a second signature dependent upon both the current user identity and the current user system in combination. The certifying system then compares the second signature with the first, as stored, to certify the transaction. The certification can accommodate normal computer system component drift. An inquiring system, desiring to confirm the identity of a user, issues a challenge code to the user system. The user system then digests the user's PIN, individual component signatures as they currently exist on the user's system, together with the challenge code to generate the new signature. The new signature is transmitted back to the

inquiring system, which transmits it on to the certification server together with the challenge code. The certification server then digests the challenge code with the original signature as previously stored, and compares the result to the newly provided signature to confirm the users identity, else drift criteria can be applied if desired.

With respect to claim 20, claim 20 depends from claim 19 and Applicant respectfully submits that claim 20 is allowable over Angelo in view of Arbaugh and further in view of Stallings for at least the reasons discussed above with respect to claim 19. LeBourgeois is not cited as curing, and does not cure, the deficiencies of Angelo in view of Arbaugh and further in view of Stallings discussed above with respect to claim 19. Accordingly, for at least these reasons, Applicant respectfully submits that claim 20 is allowable over Angelo in view of Arbaugh and Stallings and further in view of LeBourgeois.

Applicant respectfully requests that the §103 rejections be withdrawn.

Conclusion

Claims 1-21 are in condition for allowance. Applicant respectfully requests reconsideration and issuance of the subject application. Should any matter in this case remain unresolved, the undersigned attorney respectfully requests a telephone conference with the Examiner to resolve any such outstanding matter.

Respectfully Submitted,

Date: 1/31/06

By: _____

Allan T. Sponseller
Reg. No. 38,318
(509) 324-9256